pan-European Management of Biological toxin incidents through standaRdisAtion initiatives for Crisis response Enhancement

# D1.2
# DATA MANAGEMENT PLAN
# FIRST ITERATION

Funded by the European Union

EMBRACE is funded by the European Union's Horizon Europe Research and Innovation funding programme, Grant Agreement N° 101168322.

| | |
|---|---|
| **Lead author(s)** | Susan Denham (TEL), Julia Rieger, Kurt Zatloukal (MUG) |
| **Lead beneficiary** | TEL |
| **Status** | Submitted |
| **Version** | 1.0 |
| **Due Date** | 31/03/2025 (EU submission) |
| **Delivery Date** | 31/03/2025 |
| **Dissemination Level** | PU |
| **Work Package** | WP1. Project management, quality assurance, ethical and legal issues |
| **Task** | T1.4 Social, Legal, and Ethical management |
| **Contributors** | Jonathan Hall, David Crouch (RAN) |
| **Reviewers** | Mario Amo (MION), Maria Elena Dimitrakopoulou (TEL) |
| **Language** | English |
| **Format** | .pdf |
| **Keywords** | Open data, FAIR principles, reuse, interoperability, security, data protection |
| **Abstract** | The first iteration of the EMBRACE Data Management Plan provides an overview of the expected data assets of EMBRACE and the principles and methods which will be adopted to ensure FAIR access to the data, as well as protection of sensitive data. |
| **Reference this document** | EMBRACE_ D1.2 Data Management Plan - First Iteration_TEL_Version_1.0 |
| **Disclaimer** | The information and views set out in this publication are those of the author(s) and do not necessarily reflect the official opinion of the European Communities. Neither the European Union institutions and bodies, nor any person acting on their behalf, may be held responsible for the use which may be made of the information contained herein. |

## Revision history

| Version | Date | Partner | Description / Modification |
|---|---|---|---|
| 0.1 | 06/01/2025 | TEL | Table of Contents |
| 0.4 | 04/03/2025 | MUG | Complete draft |
| 1.0 | 26/03/2025 | TEL | Revisions to draft in response to reviewers |

## Abbreviations

| | |
|---|---|
| CMINE | Crisis Management Innovation Network Europe |
| DMP | Data Management Plan |
| DPO | Data protection officer |
| EAB | Ethics Advisory Board |
| EC | European Commission |
| EPG | EMBRACE Project Guide |
| FAIR | Principles to ensure that digital assets are Findable, Accessible, Interoperable, and Reusable. |
| GDPR | General Data Protection Regulation |
| PID | Persistent Identifier |
| R&D | Research and Development |
| RO | Research Organisation |
| SAB | Security Advisory Board |
| SEN | Sensitive information or data, with dissemination and sharing restricted to the consortium and the EC |
| WP | Work Package |

## Table of Contents

## Tables

# 1 INTRODUCTION

## 1.1 Overview

The EMBRACE Data Management Plan (DMP) describes the management of data that will be processed during the project (pre-existing and newly generated data). It defines a framework for complying with FAIR[1] data principles, as well as the procedures for protecting any sensitive data that is identified. This is a "living" document that will be updated throughout the project duration.

## 1.2 Purpose and Scope

The organisation of this document is structured according to the Horizon Europe Data Management Plan template[2]. Key questions it addresses include what type(s) of data the Action will collect/generate, what the applicable data standards are, how this data will be made accessible for verification and re-use, and how the data will be curated and preserved during and beyond the end of the project. Elements of the document, principally the data definitions and descriptions, will be held in a dynamic state, and the document itself will be periodically updated.

## 1.3 Structure

This document is structured as follows: Section 2 summarises the data that is expected to be generated by the project, Section 3 outlines the data governance procedures adopted by EMBRACE, Section 4 describes procedures for ensuring compliance with FAIR policies, Section 5 describes how FAIR principles will be respected for other project outputs (i.e., those that are not simply data), Section 6 discusses dual use assessment, Section 7 addresses data security, including provisions for SEN data, Section 8 outlines the project's ethical code of conduct with an explanation of how it will be implemented, Section 9 describes the resources devoted to data management, while Section 10 wraps the main document up. Annex A lists the EMBRACE beneficiaries, Annex B provides details of the Data Protection Officers nominated by each partner, and Annex C presents details of the data expected to be gathered/generated by EMBRACE, organised by Work Package.

## 1.4 Document review schedule

This document, as indicated by its title, presents an initial version of the project's Data Management Plan (DMP), based largely on partners' expectations of their data assets. The document will be maintained as a living document, subject to scheduled 6-monthly updates. Any new data assets identified by partners during each 6-month period will be integrated into the new version of the document. D1.3 with a deadline near the end of the project will contain the Final version of the project's DMP.

[1] Principles to ensure that digital assets are Findable, Accessible, Interoperable, and Reusable.
[2] https://www.openaire.eu/images/Guides/HORIZON_EUROPE_Data-Management-Plan-Template.pdf

# 2 SUMMARY OF EMBRACE'S DATA ASSETS

According to the Horizon Europe data management guidelines, the term data assets is intended to be broad and inclusive. In EMBRACE, therefore, the data assets that we consider include, for example, interviews, surveys, trial evaluation and workshop results, personal data of workshop participants, personal data of sample donors and field trial participants, expert registries, instrument recordings, as well as procedures, software, workflows, protocols, models, and physical outputs (e.g. new materials, antibodies, reagents, biological samples, and organ cultures).

EMBRACE will generate data through research studies performed in each work package (WP) of the project. These data will be managed exclusively by the respective Research Organisations (ROs) responsible for the data asset and their own professional networks, each with their appropriate ecosystems. In WPs when one or more partners will work with data generated by another partner, they will agree in advance on the applicable quality standards, reporting, format, and conditions for further use. EMBRACE will also generate and process data for management purposes.

The main data groups are:

- Data on beneficiaries and participants in project events used to support project management and community building activities
- Reuse of pre-existing data for executing the research and development (R&D) work, primarily arising from prior research but also from collaboration agreements with other organisations and projects
- Data generated by performing the R&D work of the project, primarily instrument recordings, and operational and analytical procedures, solution evaluations during experiments and field trials, and software tools and systems.
- Data on sample donors and volunteers participating in field studies
- Physical data assets such as tissue samples, short term organ cultures, biotoxin reference materials and simulants.

The project builds on the expertise of existing ROs in the field of biotoxins, their detection, analysis, and decontamination, as well as first responder protection measures, forensic investigations with sample and casualty tracking, and an extensive network of collaborators and collaborating organisations. Reuse of data is at its very core. Each of the organisations has its own data management plan or equivalent documents. For the purposes of EMBRACE, however, the organisations have agreed to share this plan which defines the data management practices that will apply within the project.

EMBRACE's primary goal is to improve Europe's capability and capacity to respond decisively to a biotoxin incident by fostering a thriving and sustainable biotoxin-responder community, capable of a comprehensive response to a biotoxin disaster. This involves ensuring the interoperability of services and data, and adhering to FAIR principles, especially in terms of interoperability and reusability. For these reasons, partners will seek to maximise the reusability of their data while improving innovative solutions and protocols specific to biotoxin incidents.

The size of the data assets at this early stage of the project is not yet clear. However, each organisation will provide appropriate data services and facilities considering the needs of the research activities to be undertaken. The origin of each data asset will generally depend on the RO, as indicated in the data asset tables in Annex C. Additionally, there may be other external sources (e.g. contextual data) providing access to pre-existing databases and/or data to be used for analysis processes.

Our intention is that this document should help to increase data availability and potentially ignite further research to expand knowledge in the field of biotoxins. Increased data reuse will benefit not only the data consumers but also the primary data generators, whose work will be amplified through data reuse.

# 3 DATA GOVERNANCE

Data governance in EMBRACE focuses on ensuring effective management of all data assets used by and generated in the project.

EMBRACE's data governance framework is structured to support accessibility, quality, ethical principles, privacy and security. Accessibility is assured by compliance with FAIR data principles[3]. Data quality is supported by the quality management approach adopted for all deliverables, and detailed within D1.1, the EMBRACE Project Guide (EPG)[4].

EMBRACE has appointed a Security Advisory Board (SAB) to advise on measures for protecting sensitive information. Procedures for protecting such information are described in the EPG, section 7.3 and are elaborated in section 7 of this document.

All data which involves human participants or samples is strictly controlled by adherence to national ethical regulations and the General Data Protection Regulation (GDPR)[5], and such data will be collected only after ethical scrutiny and approval by national ethics boards. Ethical compliance will be overseen by EMBRACE's Ethics Advisory Board (EAB). Secure data storage within the facilities of consortium partners will ensure that the data is properly protected, and access to the data is controlled, as necessary. Where possible data will also be made available through well-respected repositories such as Zenodo[6]. Ethical and Legal Guidelines for work in EMBRACE are contained in Section 8 of the EPG and in this document.

## 3.1 Data Management Roles and Responsibilities

Each partner has a role to play in the context of data management, as summarised in the table below.

| Group | Data | Responsibility |
|---|---|---|
| Data Protection Officers | Information about human participants | Advice on GDPR compliance and rights of human participants |
| EAB | Data involving human participants human or biological samples, and medical data | Review ethical applications, advise on ethical issues related to the data |
| SAB | All sensitive information | Review information, advise on security classification, dual use assessment and controls, *etc* |
| Data producer | Various | Share data as openly as possible, while respecting security restrictions. |

[3] The FAIR Guiding Principles for scientific data management and stewardship | Scientific Data
[4] https://stage.embracebiotoxhub.eu/materials/public-deliverables
[5] https://gdpr-info.eu/
[6] https://zenodo.org/

| | | |
|---|---|---|
| | | Keep any data labelled SEN secure, and only allow access to the data to members of the consortium or the EC on a need-to-know basis |

***Table 1. Summary of data governance responsibilities***

### 3.1.1 Partner Data Protection Officers

In accordance with **Article 37** of the GDPR, a data protection officer (DPO) has been appointed by each partner who conducts activities involving human participants (see Annex B). The DPOs are responsible for advising their organisations on GDPR compliance regarding the rights of participants over their personal data and the protection of personal data.

### 3.1.2 Security Advisory Board (SAB)

A Security Advisory Board (SAB), coordinated by Hanna Hakulinen (VER), has been established. The role of the SAB is to review study plans and project outputs, including data, to assess whether they include any security sensitive information, and to introduce timely measures for protecting sensitive data and preventing the dissemination of sensitive information.

| Member | Partner | Professional role | Areas of competence | Country |
|---|---|---|---|---|
| Hanna Hakulinen | VER | VERIFIN Director | Chemistry | Finland |
| Vít Střítecký | TPEB CR | Associate Professor in International Security | Security | Czech Republic |
| Daoíz Zamora | MION | Industrial & control engineer | R&D, engineering | Spain |
| David Crouch | RAN | University professor, Company director | Counter-CBRN, standardisation | United Kingdom |

***Table 2. The Security Advisory Board***

In summary, the SAB will have a proactive advisory role, with responsibilities that include identifying sensitive information produced by work in EMBRACE and ensuring proper protection of sensitive information.

The following procedures have been implemented to support these goals with respect to data produced in EMBRACE:

a) Before any data may be uploaded to a public repository submission, a description of the data, with assessment of potential security issues, must be submitted to the SAB.
a) The SAB will be responsible for checking the data to decide whether all or part of the data should be considered as sensitive.
b) Any data designated as sensitive must be removed from the data asset before it may be uploaded to any public space.
c) All sensitive data must remain confidential to the consortium and the EC.
d) Decisions about data sensitivity and steps required for protection of the identified sensitive data will be recorded in the project management system, Teamwork, in conjunction with each

submission of a submit a Security Clearance Request form. These procedures described in the EPG, section 7.3.

### 3.1.3 Ethics Advisory Board (EAB)

Ethical and legal issues related to the work performed within EMBRACE refer to the use of human biological samples and associated medical data, as well as the participation of people in the performance of experimental studies, field trials and evaluations. The **Ethics Advisory Board (EAB)**, coordinated by MUG, will be responsible for overseeing ethical and legal matters in EMBRACE. The board consists of an internal group, represented by partner institutions, complemented by two independent external experts.

| Member | Partner | Professional role | Areas of Competence |
|---|---|---|---|
| Kurt Zatloukal | MUG | Secretarial assistance to the EAB | Former member of the Ethics Board of the Federal Chancellery of Austria |
| Hannes Kern | DCNA | Scientific coordinator | CBRN, Industrial hazards, First responders |
| Danka Foitik Schmidt | ARC | Manager, Psychotherapist | Disaster management, First & Second responders |
| Iliana Korma | PUI | EU Project Coordinator | Research and development, First & Second responder |
| András Dinnyés | BIOT | General Director | Ethics of human stem cells, samples, 3Rs, EU ethics reviewer |
| Josef Haas | External 1 | Ethics expert | Former chair of the Ethics commission at the Medical University of Graz |
| Emmanuelle Rial-Sebbag | External 2 | Research Director, Lawyer | Leading European ethicist |

***Table 3. The Ethics Advisory Board***

In summary, the EAB will have a proactive advisory role, with responsibilities that include:

- Identifying project activities or results that might raise legal, ethical, societal or security concerns.
- Receiving reports from the DPOs to monitor compliance of project activities with ethical and legal requirements of the GDPR.
- Reviewing the DMP to ensure that it clearly identifies and describes the data protection measures and procedures relevant to project activities.
- Liaising with partner DPOs to oversee appropriate implementation of data rights and protection procedures and protocols.
- Initiating consultations with the Security Advisory Board (SAB) to consider specific security related concerns with regard to any data asset, as the need arises.

### 3.1.4 Data Producers

Data producers will undertake to share their data as openly as possible, while respecting, security, ethical, legal, and valorisation concerns. In all cases the data producer will be responsible for storing the data securely. In the event that a data asset is not to be released to the public, then the data producer must respect the specific access restrictions imposed on the data. For example, SEN data may only be shared with members of the consortium and the EC on a need-to-know basis, and any access to the data must be monitored.

# 4 FAIR DATA

## 4.1 Making data findable, including provisions for metadata

Data managed through EMBRACE ROs and related networks will use and prioritise persistent identifiers (PIDs) generated in their systems. The identifiers will comply with schemas that are well recognised by the relevant scientific communities. Each PID will lead to a landing page where information about the data, including related publications, citation recommendations, data use policy, and a download link will be provided, as necessary.

EMBRACE also generates and manages data for management purposes that too will be identified by PIDs. This identification process, originating in the scientific activities carried out within the framework of EMBRACE, will ensure that each data asset has an unambiguous PID, and will be extended to include all digital objects generated or managed by EMBRACE. As far as EMBRACE deliverables are concerned, the following document identifier template has been defined:

EMBRACE_Dx.y <deliverable title>_<lead partner acronym>_Version_<version number>

The landing page for all EMBRACE deliverables is

https://embracebiotoxhub.eu/materials/public-deliverables\

The use of metadata, i.e. data about data, is intended to provide information about a data asset[7], e.g., content, quality, format, access rights, etc. Metadata can take many different forms, including free text, and structured data with standardised formats. Metadata is primarily intended to promote the discovery and reuse of data assets. The most common categories of metadata are: descriptive data (required for data discovery and assessment), provenance data (describing the origins and processing of the data), technical data (defining the data formatting, database configuration, licensing information, etc), preservation data (information on how the data is maintained for longevity), and citation metadata (information needed for users to cite the data). Each EMBRACE data asset will be associated with metadata, according to a schema appropriate for the specific data type. For example, mass spectrometry data arising form the analysis of biotoxins will use the MIAPE-MS metadata standard[8], while other data assets will conform to the DCAT[9] metadata standard, specifically designed to promote interoperability between data assets available on the web.

For each data asset, we propose to apply a metadata standard according to the needs of the specific type of data. Each data producer will notify the relevant WP Leader of this decision. In a next step, we will review the metadata recommendations to consider when and how these metadata have to be provided to increase interoperability. In the case of data held in public platforms, enrichment systems will be proposed to each stakeholder to increase interoperability and findability of EMBRACE data assets, e.g., by using the categorisation system for data in the Life Sciences[10]. Through regular consultation with all WPs and involved partners, the EMBRACE DMP leaders will initiate a process to formulate a metadata schema for EMBRACE, which defines which metadata must, should, or may be provided for each type of data asset / related digital object. The focus will be on using metadata to

[7] https://ardc.edu.au/resource/metadat

[8] See: https://www.psidev.info/miape

[9] See: https://www.w3.org/TR/vocab-dcat-3/

[10] An iterative and interdisciplinary categorisation process towards FAIRer digital resources for sensitive life-sciences data, David, R., et al, Nature Scientific Reports (2022) 12:20989

promote discovery and reuse by other stakeholders.

Only public metadata validated by adequate ROs will be able to be indexed by intercommunity data portals. In addition, some EMBRACE metadata may be partially qualified as sensitive (or even classified) by authorised stakeholders and will be only harvested internally and/or by RO systems to be indexed in protected catalogues. Upon publication of data in public repositories, the appropriate metadata as required by these repositories will be linked to the data assets that are being made public.

## 4.2 Making data accessible

EMBRACE data assets designated PU will be made public through entrusted repositories. Each RO participating in EMBRACE uses repositories appropriate to their specific needs and the type of data that they generate/use. Most ROs have established and well-defined solutions. When a partner does not have sufficient experience, consortium experts will support these partners to leverage FAIR data principles and the use of Core Trust Seal[11] certified repositories. A harmonisation of repository choice, depending on identified discrepancies between data services carried out for different partners on the same type of data, will be provided in the final version of this DMP. Public repositories will be assessed for each data asset as it approaches the point of being made public, e.g. in the context of a joint publication.

Each partner, guided by the SAB and the DPOs, will have to decide for each of their data assets, whether it should be made publicly available or not, considering its sensitivity, following the principle of "*as open as possible, as protected as necessary*"[12]. The definition of levels of sharing (anonymisation, partial data, embargo) is supported by the relevant community, and applicable regional laws. For example, MUG will process personal data from patients who have given informed consent that their medical data and surgically removed organs can be used in the context of the research activities of EMBRACE. The use of this data is specified by the informed consent agreement and the approval for the study by the research ethic committee. Only anonymized data can be shared.

Rules for data embargos are defined by each partner institution. Those who do not have defined rules will be supported by experts from relevant communities and ROs, and by the EMBRACE DPOs to apply best practices. In the context of the discovery and development of new technologies and/or devices, data cannot be released until publication of a patent application. Only after protection is secured, can data be released in the form of posters, presentations, scientific manuscripts, or databases.

As far as possible, data provided will be accessible through free and standardised access protocols. When not yet available, the implementation of access protocols will be supported by experts from relevant communities to apply best practices. Publicly available data will be accessible through public data repository platforms. However, there will not be any uncontrolled access to partner databases.

Some participating organisations hold restricted, classified or sensitive data. Data access information will be provided alongside the data. For example, personal patient related data processed by MUG are restricted in their use according to informed consent and research ethics committee approval. Patient related data can only be shared in an anonymized manner. To support the sharing of such

[11] https://www.ccdc.cam.ac.uk/about-us/accreditation-and-policies/coretrustseal/
[12] https://openscience-ipr.eu/as-open-as-possible/

data, EMBRACE will investigate the use of the tools and recommendations of the EOSC-Life project[13]. In addition, access to this data will be monitored. Participating ROs have their own rules and processes for ascertaining the identity of any persons accessing their data assets. All those wishing to access data will be put in touch with the persons responsible for running these processes, assuring proper identity determination and confirmation. ROs, may if necessary, create data access committees to regulate data access.

Most of the participating ROs strive towards data sharing with Creative commons license (CC0)[14] or at least a CC-BY licence (i.e., in which any use of such data must acknowledge the creator of the data), if they are not subject to commercial constraints. In addition, some data sharing will be limited by ethical or legal aspects.

Single tools typically cannot be guaranteed to be maintained in the long run, even though each RO is expected to be sustainable in the long term. EMBRACE's sustainability plan addresses the issue of longevity though close involvement with the CMINE and CSTAC communities, and the newly established Disaster Risk Stakeholder Hub[15], with the goal of making tools and data assets available to the community for further development over the longer term. The benefit of this approach is exemplified by the data sharing agreement with the PEERS project (Grant Agreement No. 101074040), which will enable EMBRACE to build upon prior work on constructing a CBRNe knowledge hub to include new biotoxin related material. The aim is to share the biotoxin-extended knowledge hub with the community in an effort to facilitate collaborations to build ever more powerful and comprehensive knowledge tools.

In general, data that are stored in databases are accessible through well-defined and maintained database platform software. In addition, participating ROs may require the use of standardised and well-documented access protocols, which may be implemented in the form of software tools, to provide access to their data. All necessary data access tools will be validated within EMBRACE, and relevant usage and download information will be provided.

## 4.3 Making data interoperable

Data and metadata standards are needed to achieve a common understanding of data assets, thereby facilitating interoperability, comparability, discoverability, and data aggregation[16]. Some EMBRACE partners occupy key roles in managing access to scientific data or metadata, with varying approaches to interoperability and data sharing. Each EMBRACE activity will indicate in its data management plan, or equivalent document, how interoperability will be promoted. Partners will also be encouraged to apply recommendations provided by other EC projects on crisis management of biotoxin incidents.

[13] https://www.eosc-life.eu/

[14] https://creativecommons.org/share-your-work/cclicenses/

[15] https://www.cmine.eu/topics/35391/page/home

[16] https://open-data-institute.gitbook.io/data-governance-playbook/play-four-making-data-interoperable/standards-for-data-and-interoperability

From the outset, EMBRACE has adopted and made public, a standardised Glossary of Terms[17]. This comprehensive glossary of CBRNe terms has been compiled through work in prior projects and the following organisations:

- International Standards Organisation (ISO)
- United Nations Office for Disaster Risk Reduction (UNDRR), formerly known as UNISDR and
- International Federation of Red Cross & Crescents (IFRC).

This '*Base Glossary*' of terms is the outcome of a project-specific standardisation/alignment activity that was implemented to ensure a common and sound language between researchers working on EMBRACE and for the purpose of supporting focused and comprehensive communication efforts within the project consortium and with external stakeholders.

A second component of the glossary is the '*Project Glossary*'. This includes those terms and phrases that are either: previously used in Horizon-funded research projects new to the Disaster Resilient Societies world due the specialist activities of EMBRACE or accepted terms from the Base Glossary which need 'flexing' to fit the activities and context of our work.

Development of the Project Glossary is ongoing and should be considered as 'work in progress'. It will be kept live for the entire duration of the project as new entries are proposed, and the EMBRACE consortium stresses and tests its own explanations and definitions. The Project Glossary will become increasingly credible as time progresses and will be completed for publication towards the final stages of the project. At this stage of the project, the majority of terms presented have been identified through the research efforts employed through Work Package 2, creation of the Biotoxin Task Force. It is expected that terms may be removed or newly defined as the project continues.

The EMBRACE project is keen to deliver value beyond its original remit, in particular to other projects operating within the Disaster Resilient Societies area and represented in the CBRNe and Standardisation Cluster of projects known as CSTAC. This will be achieved through developing and sharing the 'Base Glossary' with all collaborating projects and by sharing the evolving EMBRACE 'Project Glossary' to avoid duplication and encourage academic consideration and challenge of the definitions or meanings selected.

In summary, EMBRACE will seek to identify biotoxin-related gaps in the base glossary to provide proposed terminology additions/refinements that will be shared with the community. Wherever possible, data assets will use terminology drawn from standard ontologies, including the EMBRACE Glossary of Terms. Where this is not possible, the corresponding gap will be identified, and new terminologies proposed. Any usage of ontologies will be carried out with the utmost care to avoid proliferation of confusion caused by inappropriate or contradictory use of terms. In addition, partners will be encouraged to include qualified references in data assets at each step of data production and harmonisation, as a minimum through metadata aggregation and platforms.

[17] https://embracebiotoxhub.eu/glossary

## 4.4 Increase data re-use

Some ROs of the EMBRACE project are actively involved in developing means for improving data reuse, specifically through increasing the reproducibility of analytical results that will be used within the project, including methods for data cleansing and data harmonisation. These efforts will be discussed with partners engaged in collaborative tasks as a first step.

Project documentation will be public as far as is feasible and acceptable to the partners. For example, with the exception of early drafts, successive versions of this document will be available on a file server, grouped in a single directory in order to provide simple accessibility.

The EMBRACE project will comply with Horizon Europe's open science expectations and ethos. The participating ROs strive towards the widest distribution of data possible, while taking into account their own commercial and other related strategic priorities. All data will be, by default, open, unless there is a legitimate reason to restrict access to some or all of it (e.g., some chemical structures may be considered as sensitive and/or non-sharable, or biotoxin protocols may be withheld in respect of dual use considerations). Experimental data sets will be archived in repositories with DOI numbers for findability and publication purposes. Images and their metadata (image pixel size, objective and experiment details, time/date, and detailed acquisition parameters) as well as all -omics data will be accessible and processable by open-source programs. The consortium will also share any manuscript (without a legitimate reason to restrict access to some or all of it, see above), on preprint servers such as bioRxiv[18] to accelerate access to findings for the whole scientific community.

The consortium will provide immediate open access to all its scientific publications (peer-reviewed or not) and will prioritise providing systematic Open Access to publications through either the green (publication in a subscription-based journal, with a copy of the article placed in an institutional repository), or the gold route (publication in an open access journal).

Reuse by third parties will be promoted by the efforts of participating ROs towards the most sustainable distribution of data possible. This will ensure that data is reusable beyond the end of the project in all legal contexts validated by appropriate stakeholders.

All ROs document data provenance in their resources, i.e., information about the processes and people involved in producing the data, to allow potential users of the data to form an assessment about the quality, reliability and trustworthiness of the data. Advice on the usage of provenance documentation, will be made available to all partners and EMBRACE ROs will recommend adoption of a provenance model to be used in the framework of the project[19].

Data quality assurance processes are strongly linked to communities dealing with data analyses and, in most of the cases, they are implemented during the data production processes by stakeholders in each RO ecosystem. Nevertheless, in some cases, the corresponding processes must be designed and documented in the metadata of the asset. This aspect of metadata is intended to evolve in synchrony with the DMP, in order to serve as a reference for future projects, and for the harmonisation of related data resources. Special emphasis will be placed on primary data generated within the project, e.g., by

[18] https://www.biorxiv.org/

[19] E.g., PROV-DM https://www.w3.org/TR/prov-dm/

standardisation of procedures and using reference standards as well as positive and negative controls for analytical procedures.

Each RO will take responsibility for security and ethical aspects related to their data assets, under the guidance of the SAB and EAB. Throughout the project, the data assets of EMBRACE will be mapped together with the measures adopted to ensure security and ethical compliance.

# 5 OTHER RESEARCH OUTPUTS

In addition to the research data, which is covered by the sections above, EMBRACE will generate other research outputs including revised protocols for biotoxin incident response, software tools for tracking samples and casualties, a model of first responder heat stress, a source prediction model, and a range of software programmes needed to support and achieve the task results identified in the DOA. EMBRACE will also generate a number of physical objects including tissue samples, 3D brain models and other short term organ models, biotoxin simulants, and biotoxin reference samples, and reactants. Where possible, these assets will be made publicly. However, it is likely that many of them will be regarded as commercially or security sensitive and not suitable for public sharing. Each of these non-standard assets will be identified as they are created, and a decision will be made regarding their status following the consideration and advice of the SAB and EAB.

# 6 DUAL USE ASSESSMENT

EMBRACE will be processing, and possibly sharing, information, software, data, materials and devices that fall under dual use regulations[20]. For example, biotoxins such as Ricin are considered as chemical weapons under the Chemical Weapons Convention. Ricin is a controlled chemical under Schedule 1A of the Chemical Weapons Convention (CWC) and is a Category B substance under the Biological and Toxins Weapons Convention (BTWC)[21]. Therefore, dual use assessment of the work performed within EMBRACE, including all associated data and information is mandatory.

Under EU and the aligned UK export control regulations[22] EMBRACE must not export[23] any items that may be used in relation to chemical, biological or nuclear weapons. Within this context there are controls over the transfer of software or technologies within and outside of the EU to another country. EMBRACE will potentially be producing items of concern, including for example detection systems, decontamination and PPE procedures, biotoxin incident scenarios and response CONOPs, etc.

The SAB will oversee dual use assessment of project outputs, and a plan for carrying out this work will be agreed with the Project Officer. The draft plan is as follows:

a) For each task determine what items may potentially be subject to dual use regulations.
b) Document each such item, including a description, details of ownership, organisation(s) with whom it needs to be shared, and proposed data protection measures.
c) Consult with national contact points determined by ownership of the item. This is necessary as there is no European process that pertains to all countries, and individual countries may have regulations in addition to those in force across the EU.
d) In the event that a project item becomes subject to dual-use regulations, necessary steps will be taken to ensure compliance with the relevant regulations as advised by the regulatory authority.

In carrying out this plan, EMBRACE will follow both EU[24] and national recommendations on exporting dual use products and technologies. The key messages from these documents is that "Dual-use items may be traded freely within the EU, except for some particularly sensitive items, whose transfer within the EU remains subject to prior authorisation" (Annex IV of the Regulation). In addition, "In certain cases, EU Member States may introduce additional controls on non-listed dual-use items because of public security or human rights considerations". For this reason, the partner responsible for a specific item in question will be required to consult their national contact point to find out whether there are additional controls on non-listed dual-use items applicable in their country.

[20] https://eur-lex.europa.eu/EN/legal-content/summary/dual-use-export-controls.html
[21] See https://www.opcw.org/sites/default/files/documents/SAB/en/sab-21-wp05_e_.pdf
[22] See https://www.gov.uk/guidance/export-controls-dual-use-items-software-and-technology-goods-for-torture-and-radioactive-sources#dual-use-items-software-and-technology
[23] As 'export' applies to the transfer of an item between countries, export restrictions will apply to the transfer or sharing of restricted items between partners from different countries.
[24] https://policy.trade.ec.europa.eu/help-exporters-and-importers/exporting-dual-use-items_en

Questions over the EU policy on the identification and transfer of dual use-controlled items, as might arise from EMBRACE activities, are currently being considered in consultations between the SAB and the EMBRACE Project Officer and her legal team. This section will be revised once these issues are clarified.

# 7 DATA SECURITY

EMBRACE data assets will be stored by individual partners and in the project repository. Access to the repository is only available by invitation of the Project Coordinator. The repository essentially provides a moderately secure space for storing data, and for avoiding accidental loss. Partners will also be encouraged to ensure that the data security procedures in their organisations are fit for purpose.

In the event that sensitive data is identified, access to this data will be restricted, and protected by end-to-end encryption, with access carefully controlled using specific permissions. Secure storage of the sensitive data will be the responsibility of the lead partner responsible for the generation and processing of the data. Details of the procedures for protecting sensitive data, approved by the SAB, will be communicated with the responsible partners. The security policy of EMBRACE is covered in section 7 of the EPG.

As EMBRACE deals with biological toxin incidents and crisis response management, there are reasonable security concerns associated with some of the data assets. During the negotiations, a number of deliverables were identified as potentially containing sensitive (SEN) information. Any document or data labelled as SEN cannot be disseminated to third parties not listed in the DoA without prior authorization from the granting authority. Data associated with these deliverables will be carefully considered by the SAB before permission to allow access can be given.

For SEN data, beneficiaries may disclose sensitive information to their personnel or other participants involved in the action **only** if they (cf. Art 13.1 of GA):

(a) need to know it in order to implement the Agreement, and

(b) are bound by an obligation of confidentiality.

To ensure compliance with these requirements, the responsible beneficiaries will be required to explicitly audit access to SEN data and put in place confidentiality agreements before granting access.

All parties must keep confidential any data, documents or other material (in any form) that are identified as sensitive in writing ('sensitive information') during the implementation of the action and for at least 5 years after final payment.

# 8 CODE OF ETHICS

## 8.1 Guidelines for Ethical Data Handling

Numerous publications exist on the topic of ethical data handling. In EMBRACE we adhere to the following general principles regarding data usage:

1. The data has clear benefits for users and serves the public good.
2. The data subject's identity (whether person or organisation) is protected, information is kept confidential and secure, and the issue of consent is considered appropriately.
3. The data processing methods employed are consistent with recognised standards of integrity and quality.
4. Data usage, processing and storage are consistent with legal requirements including the General Data Protection Regulation.
5. The views of the public are considered with respect to the data and the perceived benefits of the research.
6. The access, use and sharing of data is transparent, and communicated clearly and openly.

## 8.2 Ethical Principles and Considerations

Compliance with the GDPR and the ethical and data protection standards set out by the European Commission is essential. All partners are required to adhere to these regulations and standards. In instances of joint data management, the partners responsible for such data will define their respective responsibilities through an agreement, which will be made accessible to all participants.

In compliance with the GDPR, the following rights of participants will be ensured:

1. The right to know what personal data will be collected, how it will be used, and who can access it.
2. Participants will be required to provide informed consent to the use of their data, without which such data may not be used. Participants will also be informed on their right to withdraw consent, and procedures for doing so.
3. Participants have the right to access their personal data and to specify corrections.
4. Participants have the right to be forgotten, i.e., deletion of their personal data.
5. Partners are responsible for the implementation of appropriate measures to protect all personal data gathered from unauthorized access or alteration.
6. Participants have the right to lodge complaints with data protection authorities if they believe their rights have been violated.

## 8.3 Protection of personal data

As far as possible EMBRACE will avoid the use (collecting, processing, and storage) of personal data, opting instead to pseudonymize or anonymise all such data. Where this is not possible EMBRACE will ensure that the use of all personal data is carried out strictly in accordance with the General Data

Protection Regulations, defined in Regulation (EU) 2016/679 including the implementation of measures to ensure the protection and confidentiality of personal data.

Various project activities involve human participants, including research studies, interviews, project events, workshops, and evaluation trials. To comply with European regulations on data privacy and protection, all studies involving human subjects will be require prior approval by a research ethics committee and participants will always be requested to sign informed consent forms, giving them the option to accept or refuse the use of their personal data and any images in which they appear. Templates of informed consent forms and information sheets are provided in the project repository. Hard copies of consent forms and any identifiable data will be kept in locked drawers. Digital versions will be stored locally, encrypted and protected according to the internal procedures of the responsible partner. Only authorized people will have access to such data.

# 9 DATA MANAGEMENT RESOURCES AND TOOLS

## 9.1 Allocation of resources

As it is anticipated that some data assets managed by EMBRACE may be classified as sensitive, there is provision in the budget for ensuring the protection of sensitive data, including secure storage, and secure data transfer between those with the need and right to access the data.

## 9.2 Repository

The EMBRACE coordinator (TEL) has established a project management framework and repository using Teamwork, an integrated project management system that allows partners to manage and schedule project activities, share and exchange documents, gather data using forms, and much more. This repository serves as a central location for storing and sharing project information, materials and files. Additionally, the web-based platform offers additional functionalities, which are detailed in the Annex C of the EMBRACE Project Guide. Access to the repository is limited to designated staff members from consortium partners, who must be explicitly invited by the coordinator. The repository benefits from continuous backup, ensuring that each document uploaded to the system is securely held.

In the event that sensitive data is identified, a more secure solution which uses a virtual private network (VPN) with end-to-end encryption, together with secure storage will be implemented. One possible European vendor being considered is Nord-VPN as it offers:

- Meshnet: a means for creating a secure private communications network to link up to 60 devices. Once connected, the devices act as though they were on a local area network (LAN) and are able to securely send files directly to each other.
- NordLocker cloud storage: in which all items are protected by end-to-end encryption as they are added to the vault, with the facility to allow the owner to give others access to specific files.

The final decision on secure storage will be taken by the SAB once the scope of the problem has been established.

Other repositories that will be used by EMBRACE, principally for making data assets available to the community include:

- Zenodo (a general-purpose open-access repository developed under the European OpenAIRE program).
- CMINE's Disaster Risk Stakeholder Hub.
- A publications' download page on the project website

## 9.3 Data Preservation

A strategy for ensuring preservation of data assets beyond the funding duration of EMBRACE will be formulated. At the very least, project data will be retained for 5 years after the project's conclusion within Teamwork. After this, data will be transferred to servers where it will remain accessible to consortium members. The majority of the data assets will in any case be preserved through the use

of open repositories, e.g., Zenodo, where all project outputs that are not sensitive will be held. To further preserve project outcomes, all results deemed to be of sufficient potential interest to others in the community will be offered to the community using CMINE's **Disaster Risk Stakeholder Hub**.

# 10 CONCLUSION

This initial version of the Data Management Plan (DMP) is a first step towards a comprehensive DMP for EMBRACE. This plan defines a framework for efficient and responsible handling of research data, ensuring compliance with ethical, legal, and regulatory requirements. EMBRACE has been formulated to respect the principles of open science, transparency, and collaboration and will strive to ensure that its results are shared with the community. To maximise the impact of its work EMBRACE will carefully adhere to FAIR data principles, making data findable, accessible, interoperable and reusable. The plan also identifies the tools and resources necessary for effective data management, and means for ensuring data integrity, accessibility, and long-term usability. Robust security measures are proposed for protecting personal and other sensitive data. The DMP is a live document that will be regularly updated to provide researchers, collaborators, and stakeholders with clear guidelines and procedures to follow regarding data management throughout the project.

# ANNEX A. EMBRACE PARTNERS

| Partner | Partner | Acronym | Country |
|---|---|---|---|
| 1 | TELESTO TECHNOLOGIES PLIROFORIKIS KAI EPIKOINONION EPE | TEL | Greece |
| 2 | DCNA DISASTER COMPETENCE NETWORK AUSTRIA | DCNA | Austria |
| 3 | OSTERREICHISCHES ROTES KREUZ | ARC | Austria |
| 4 | POMPIERS DE L'URGENCE INTERNATIONALE | PUI | France |
| 5 | MEDIZINISCHE UNIVERSITAT GRAZ | MUG | Austria |
| 6 | HELSINGIN YLIOPISTO | VER | Finland |
| 7 | SAITAMA MEDICAL UNIVERSITY EDUCATIONAL CORPORATION | SMU | Japan |
| 8 | BIOTALENTUM TUDASFEJLESZTO KFT | BIOT | Hungary |
| 9 | AIRSENSE ANALYTICS GMBH | AIRS | Germany |
| 10 | MOBILITY ION TECHNOLOGIES SL | MION | Spain |
| 11 | PROMETECH BV | PRO | Netherlands |
| 12 | IANUS TECHNOLOGIES LTD | IANUS | Cyprus |
| 13 | THE LISBON COUNCIL FOR ECONOMIC COMPETITIVENESS ASBL | LC | Belgium |
| 14 | TECHNOLOGICKA PLATFORMA ENERGETICKABEZPECNOST CR | TPEB CR | Czech Republic |
| 15 | CESKA AGENTURA PRO STANDARDIZACI | CAS | Czech Republic |
| 16 | URAD PRE NORMALIZACIU, METROLOGIU A SKUSOBNICTVO SLOVENSKEJ REPUBLIKY | UNMS | Slovakia |
| 17 | RESILIENCE ADVISORS LTD | RAN | United Kingdom |
| 18 | BIOXHALE LTD | BIOX | United Kingdom |

***Table 4. List of EMBRACE partners***

# ANNEX B. PARTNER DATA PROTECTION OFFICERS

| Partner | Acronym | DPO | DPO email |
|---|---|---|---|
| DCNA DISASTER COMPETENCE NETWORK AUSTRIA | DCNA | Christian Resch | christian.resch@dcna.at |
| OSTERREICHISCHES ROTES KREUZ | ARC | Sandra Lichtkoppler | Sandra.Lichtkoppler@roteskreuz.at |
| POMPIERS DE L'URGENCE INTERNATIONALE | PUI | Philippe Besson | pbesson@pompiers-urgence.org |
| MEDIZINISCHE UNIVERSITAT GRAZ | MUG | Datenschutzbeauftragter | datenschutz@medunigraz.at |

***Table 5. Nominated Data Protection Officer for each partner***

# ANNEX C. DATA DETAILS FOR EACH WORK PACKAGE

The data assets expected to be managed by EMBRACE are very diverse, even within single WPs. Therefore, the data asset questionnaires completed by partners for each task, are included here grouped by WP and task number.

## WP1. Project management, quality assurance, ethical and legal issues

| Data Asset Properties | WP1 specifications |
|---|---|
| What is the purpose of data collection / generation in this WP? | Project coordination and management; Science and technology strategic steering and coordination; Data management, legal compliance, research ethics compliance; Quality Control, risk management and contingency planning. |
| What types and formats of data will be generated / collected? | Minutes, reports, guidelines, presentations, attendance sheets, Teamwork usage. Formats include: .docx, pdf, .xlsx, pptx. |
| Will existing data be re-used and, if so, how? | Yes. Data will be re-used through references / links within documents. |
| What is the origin of the data? | Project partners, stakeholders. |
| What is the expected size of the data? | To be confirmed. |
| To whom might it be useful | Project partners, stakeholders, European Commission. |
| Are these data discoverable with metadata, and identifiable and locatable by means of a standard identification mechanism? | Yes, the data can be discovered using keyword searches. |
| What naming conventions are followed? | Naming conventions for the reports are defined in the EMBRACE Project Guide. |
| Will search keywords be provided to facilitate re-use? | Yes, document control sections (will) contain keyword lists |
| Will version numbers be provided? | Yes: 0.1, 0.2 (draft), 1.0 (final). |
| What metadata will be created? | Editor, lead partner, contributors, title, date, language, format, keywords |

## WP2. Crisis management of biotoxin incidents

| Question | T2.1 |
|---|---|
| Lead Organisation | RAN |
| Data title | BTF Contacts |
| Short description | Potential members of the Biotoxin Task Force (BTF) will be recorded in the membership database in CMINE |
| Other partners involved | |
| How will the data be collected/generated/created? | Through the Hivebrite platform |
| Will you use preexisting data? | Yes, Hivebrite |
| Data format | Various |
| Tools required for accessing/using the data | Hivebrite back office |
| To whom might your data be useful outside of EMBRACE? | Nil |
| Does this data asset include any personal data? | Yes |
| What personal data will be? | Name, organisation, interests |
| What categories of persons will be included? | Professional CBRNe |
| What specific data protection requirements apply? | Bespoke requirements compliant with GDPR and SOC 1/2/3 and ISO 27001 |
| Will you use anonymisation techniques to protect personal data? | No |
| Do you comply with the requirements for valid consent? | Yes |
| Where and how will the data be stored? | Encrypted on EU Servers |
| Which partner will be responsible for controlling access to this data? | RAN |
| How will the provenance of the data be ensured? | |
| Will you use access control and/or encryption measures to protect this data? | Yes. All data is encrypted at rest by GCP using the AES-256 cipher |
| Will the data be open and reusable? | No - It is personal data and will not be made available beyond the levels stated in the consent arrangements. |
| Will this data be used for further scientific research? | Potentially but not yet |
| Will you use any metadata? If yes: which schema are you using? | No |

| | |
|---|---|
| Will you use any controlled vocabularies (terminologies, taxonomies, code lists), if so, which? | No |

| Question | T2.2 |
|---|---|
| Lead Organisation | DCNA |
| Data title | Status quo & gaps and needs |
| Short description | This is a collection of data aimed at covering current mechanisms of biotoxin management in selected EU member states and a summary of gaps and needs that are discovered during the research. |
| Other partners involved | Potentially all partners that have information to this aspect. |
| How will the data be collected/generated/created? | Desk review, interviews, workshop |
| Will you use preexisting data? | yes, we will look for publicly available data |
| Data format | Text |
| Tools required for accessing/using the data | no special tools required |
| To whom might your data be useful outside of EMBRACE? | To all interested in current developments of the biotoxin management sector |
| Does this data asset include any personal data? | This still needs to be defined. We can also agree on not collecting any personal data. |
| What personal data will be? | Name, profession, organisation |
| What categories of persons will be included? | representatives of national organisations dealing with biotoxins |
| What specific data protection requirements apply? | not yet defined |
| Will you use anonymisation techniques to protect personal data? | we have not defined a procedure yet |
| Do you comply with the requirements for valid consent? | yes |
| Where and how will the data be stored? | We are currently saving our data on the official DCNA-OneDrive. If this is not trusted, we need to find another solution. |
| Which partner will be responsible for controlling access to this data? | DCNA |
| How will the provenance of the data be ensured? | |
| Will you use access control and/or encryption measures to protect this data? | not planned. If required, we can add an additional password for EMBRACE. |
| Will the data be open and reusable? | No, the data itself will not be open as we expect a huge number of files and transcripts, but we are publishing the summary in the deliverable. |
| Will this data be used for further scientific research? | No |

| | |
|---|---|
| Will you use any metadata? If yes: which schema are you using? | No |
| Will you use any controlled vocabularies (terminologies, taxonomies, code lists), if so, which? | No |

| Question | T2.4 |
|---|---|
| Lead Organisation | VER |
| Data title | Training material |
| Short description | New training material will be create and add to the CBRN toolbox |
| Other partners involved | PCNA, MUG and PUI |
| How will the data be collected/generated/created? | Filming, taking photos, etc |
| Will you use preexisting data? | Not at the moment |
| Data format | Mostly pdf, jpeg and mpeg |
| Tools required for accessing/using the data | Web browser and corresponding software (e.g. pdf reader) |
| To whom might your data be useful outside of EMBRACE? | Mainly first responders |
| Does this data asset include any personal data? | no |
| What personal data will be? | nada |
| What categories of persons will be included? | nada |
| What specific data protection requirements apply? | username and password |
| Will you use anonymisation techniques to protect personal data? | no |
| Do you comply with the requirements for valid consent? | No personal data, so GDPR won't apply |
| Where and how will the data be stored? | Helsinki university server, data is stored in server's hard drives and random access memory (RAM) when needed. |
| Which partner will be responsible for controlling access to this data? | VER |
| How will the provenance of the data be ensured? | |
| Will you use access control and/or encryption measures to protect this data? | Username and password |
| Will the data be open and reusable? | Data is available if username and password is known |
| Will this data be used for further scientific research? | Yes |
| Will you use any metadata? If yes: which schema are you using? | No |
| Will you use any controlled vocabularies (terminologies, taxonomies, code lists), if so, which? | No |

## WP3. Detection, sampling, and identification of biotoxins

| Question | T3.1 |
|---|---|
| Lead Organisation | PRO |
| Data title | Forensics Database |
| Short description | The forensics database is the meta data and the results data of the samples which are taken at an incident scene. This is created from Tag & Trace forensics app with integrations with the detectors. |
| Other partners involved | Namely AIR and MION potentially VER and MUG could be involved as well. |
| How will the data be collected/generated/created? | Data is collected via T&T inputs, with results from AIR and MION detectors received via API |
| Will you use preexisting data? | The Tag & Trace application is pre existing and owned by PRO. |
| Data format | SQL |
| Tools required for accessing/using the data | URL and access token |
| To whom might your data be useful outside of EMBRACE? | Potential customers would be interested in the Tag & Trace forensics application |
| Does this data asset include any personal data? | User credentials like name or ID can be put in the system |
| What personal data will be? | Name, Role, ID |
| What categories of persons will be included? | Professionals |
| What specific data protection requirements apply? | |
| Will you use anonymisation techniques to protect personal data? | The user information can be anonymised for the FTXs |
| Do you comply with the requirements for valid consent? | Yes |
| Where and how will the data be stored? | Our own secure servers |
| Which partner will be responsible for controlling access to this data? | PRO |
| How will the provenance of the data be ensured? | |
| Will you use access control and/or encryption measures to protect this data? | Yes |
| Will the data be open and reusable? | Yes, the data can be shared |
| Will this data be used for further scientific research? | Yes |

| | |
|---|---|
| Will you use any metadata? If yes: which schema are you using? | No |
| Will you use any controlled vocabularies (terminologies, taxonomies, code lists), if so, which? | CAS numbers |

| Question | T3.2 |
|---|---|
| Lead Organisation | VER |
| Data title | C-MS/MS and Immunoassay-Based Biotoxin Analytics for Incident Response and Method Validation |
| Short description | This dataset consists of analytical measurements of biotoxins using liquid chromatography-tandem mass spectrometry (LC-MS/MS) and immunoassays, generated as part of an EU-funded project aimed at improving first response to biotoxin incidents. The data will support method validation, performance verification, and interlaboratory comparisons, contributing to enhanced preparedness and rapid response capabilities. Some of the validated results may be integrated into relevant biotoxin databases. |
| Other partners involved | MION, AIRS |
| How will the data be collected/generated/created? | (LC-)MS/MS and immunoassays on biotoxin samples, method validation |
| Will you use preexisting data? | Reference spectra, (bio)toxin databases, regulatory guidelines, and open-source tools. |
| Data format | Measurements as RAW, mzML, CSV, Excel, JSON; Reports PDF/Word; spectral libraries in vendor format |
| Tools required for accessing/using the data | LC-MS/MS software (Xcalibur, MassHunter), XCMS, Skyline, R, Python, database tools for integration. |
| To whom might your data be useful outside of EMBRACE? | Public health agencies, regulators, forensic labs, emergency responders, food safety authorities. |
| Does this data asset include any personal data? | no |
| What personal data will be? | |
| What categories of persons will be included? | |
| What specific data protection requirements apply? | |
| Will you use anonymisation techniques to protect personal data? | |
| Do you comply with the requirements for valid consent? | |
| Where and how will the data be stored? | Data will be stored on secure institutional servers, project repositories, and backup storage with controlled access. Zenodo, EUDAT, or an institutional repository will be used for long-term storage and accessibility. |
| Which partner will be responsible for controlling access to this data? | VERIFIN |

| | |
|---|---|
| How will the provenance of the data be ensured? | |
| Will the data be open and reusable? | Sensitive data will have role-based access control and encryption to ensure security and compliance. |
| Will the data be open and reusable? | Some data will be open-access, while others may be restricted due to biosafety/security concerns or partner agreements.<br><br>Restricted access applies to sensitive biotoxin-related datasets for security, legal, or contractual reasons.<br><br>An embargo may apply for IP protection, publication priority, or security screening, typically 6-12 months. |
| Will this data be used for further scientific research? | Data will support future studies, validation efforts, and method standardization. |
| Lead Organisation Acronym | VERIFIN |
| Will you use any metadata? If yes: which schema are you using? | Yes, DCAT or MIAPE-MS. |
| Will you use any controlled vocabularies (terminologies, taxonomies, code lists), if so, which? | Yes, ChEBI, MeSH, and IUPAC nomenclature for biotoxin classification. |

| Question | T3.3_1 |
|---|---|
| Lead Organisation | MION |
| Data title | Result data given by MION's detection technology (DMA) |
| Short description | Once a sample is introduced in the DMA for analysis, the analyzer generates a series of spectra which are internally processed. After this internal data processing which is not shared with the user, the analyzer delivers to the user the following information: 1. Code of the sample analyzed, and, 2. Result of the analysis which may be positive or negative. |
| Other partners involved | PRO. The sample must contain a "sample code" which must be read by the analyzer. |
| How will the data be collected/generated/created? | The analysis results will be shown in a screen and/or, if necessary, sent either by Bluetooth/WIFI |
| Will you use preexisting data? | In principle, it is not contemplated to use preexisting data. |
| Data format | Visual and/or .csv |
| Tools required for accessing/using the data | Visual and/or tablet or smart phone |
| To whom might your data be useful outside of EMBRACE? | The results of the analysis will be useful to first responders once the analyzer reaches the market |
| Does this data asset include any personal data? | No |
| What personal data will be? | |
| What categories of persons will be included? | |
| What specific data protection requirements apply? | |
| Will you use anonymisation techniques to protect personal data? | |
| Do you comply with the requirements for valid consent? | |
| Where and how will the data be stored? | The data will be stored in the internal memory of the analyzer. If necessary, the data can be uploaded to a project cloud. |
| Which partner will be responsible for controlling access to this data? | MION |
| How will the provenance of the data be ensured? | |
| Will you use access control and/or encryption measures to protect this data? | Yes. The user must log in to access the analyzer |

| | |
|---|---|
| Will the data be open and reusable? | The data corresponding to the analysis result can be open as long as they are not considered as restricted information by the project security committee. |
| Will this data be used for further scientific research? | If they are considered open, they will (or could) be used for further scientific research |
| Will you use any metadata? If yes: which schema are you using? | MION |
| Will you use any controlled vocabularies (terminologies, taxonomies, code lists), if so, which? | No |

| Question | T3.3_2 |
|---|---|
| Lead Organisation | AIRS |
| Data title | Measurement results from pBDi |
| Short description | The biochip-based on-site detection platform utilizes the Sandwich-ELISA principle, enabling the simultaneous detection of up to six different analytes. This platform is designed for fully automated sample evaluation and creates two files after each measurement. |
| Other partners involved | Partners involved in T3.3 |
| How will the data be collected/generated/created? | The data will be saved as .xps and .xmd files by the pBDi software |
| Will you use preexisting data? | no |
| Data format | .xps .xmd |
| Tools required for accessing/using the data | pBDi software, xps reader |
| To whom might your data be useful outside of EMBRACE? | People who are interested in immunoassays |
| Does this data asset include any personal data? | no |
| What personal data will be? | |
| What categories of persons will be included? | |
| What specific data protection requirements apply? | |
| Will you use anonymisation techniques to protect personal data? | |
| Do you comply with the requirements for valid consent? | |
| Where and how will the data be stored? | The data will be stored locally on the device used for the measurements and it will be transferred to the AIRSENSE server where only team members of the research have access to. The data is supposed to also be transferred to PRO but at the moment the details on that are not yet defined. |
| Which partner will be responsible for controlling access to this data? | AIRS |
| How will the provenance of the data be ensured? | |

| | |
|---|---|
| Will you use access control and/or encryption measures to protect this data? | yes, data can only be accessed by members of the research team |
| Will the data be open and reusable? | The data can be shared |
| Will this data be used for further scientific research? | yes |
| Lead Organisation Acronym | AIRS |
| Will you use any metadata? If yes: which schema are you using? | Yes, Open XML Paper Specification (OpenXPS) Schema |
| Will you use any controlled vocabularies (terminologies, taxonomies, code lists), if so, which? | no |

## WP4. Solutions to reduce risk and harm

| Question | T4.1 |
|---|---|
| Lead Organisation | IANUS |
| Data title | Biothreat Risk Assessment Framework Data |
| Short description | A comprehensive dataset used for the BioRA to support the modeling of toxicological effects of biotoxins. This includes trial evaluations, expert inputs, and workshop results pertaining to the toxicological profiles, response strategies, and incident management scenarios. |
| Other partners involved | MUG, TEL |
| How will the data be collected/generated/created? | field trials, expert workshops, and collaborations with laboratories |
| Will you use preexisting data? | If available, yes. DBs from partners, EU databases on CBRN management, and open-source datasets |
| Data format | CSV, JSON for structured data, and specialized formats for geographic information systems (GIS) |
| Tools required for accessing/using the data | GIS tool and programming languages for data analysis as well as databases (MariaDB, MongoDB) |
| To whom might your data be useful outside of EMBRACE? | Governmental public health agencies, other EU civil protection initiatives, academic researchers i |
| Does this data asset include any personal data? | yes |
| What personal data will be? | Names, professional roles |
| What categories of persons will be included? | Researchers, emergency responders, public health officials |
| What specific data protection requirements apply? | personal data is not accessed by unauthorized personnel |
| Will you use anonymisation techniques to protect personal data? | yes |
| Do you comply with the requirements for valid consent? | yes |
| Where and how will the data be stored? | Cloud Storage (Hetzner) |
| Which partner will be responsible for controlling access to this data? | IANUS |
| How will the provenance of the data be ensured? | |
| Will you use access control and/or encryption measures to protect this data? | YES |
| Will the data be open and reusable? | If needed, otherwise any sensitive data will be anonymised |

| | |
|---|---|
| Will this data be used for further scientific research? | yes |
| Will you use any metadata? If yes: which schema are you using? | n/a |
| Will you use any controlled vocabularies (terminologies, taxonomies, code lists), if so, which? | Yes, EPA, ISO |

| Question | T4.2 |
|---|---|
| Lead Organisation | MUG-psy |
| Data title | Stress diagnostic and resilience training |
| Short description | In preparation for the simulation, standard diagnostic procedures are used to assess the stress regulation of the first responders. This measurement then provides information about the overall stress profile of the participants. This data is collected using online questionnaires. A study code is assigned, which makes the person accessible at various test times during the study - however, the data is always processed anonymously. These study codes are in turn used for the training and assignment of the resilience training programs. The diagnosis of stress regulation after the intervention is carried out again using the same test battery and the same study code. |
| Other partners involved | Partners, who measure stress-related parameters are required for this study. |
| How will the data be collected/generated/created? | using online questionnaires |
| Will you use preexisting data? | no |
| Data format | csv |
| Tools required for accessing/using the data | Lime Survey |
| To whom might your data be useful outside of EMBRACE? | Scientists at the Medical University of Graz |
| Does this data asset include any personal data? | Yes |
| What personal data will be? | Stress processing strategies, stress regulation, mood, resilience |
| What categories of persons will be included? | fist-responder |
| What specific data protection requirements apply? | using a randomly generated and assigned study code. |
| Will you use anonymisation techniques to protect personal data? | Names are not required. The data is stored anonymously |
| Do you comply with the requirements for valid consent? | Yes |
| Where and how will the data be stored? | Password-protected on the Meduni server in Graz |
| Which partner will be responsible for controlling access to this data? | MUG |
| How will the provenance of the data be ensured? | |

| | |
|---|---|
| Will you use access control and/or encryption measures to protect this data? | Password-protected |
| Will the data be open and reusable? | No |
| Will this data be used for further scientific research? | No |
| Will you use any metadata? If yes: which schema are you using? | No |
| Will you use any controlled vocabularies (terminologies, taxonomies, code lists), if so, which? | No |

| Question | T4.5 |
|---|---|
| Lead Organisation | VER |
| Data title | VER: Analysis data |
| Short description | VER: Analysis plans. Analytical data from analytical instrumentation such as mass spectrometers. Results of data analysis. |
| Other partners involved | MUG, RAN, PRO |
| How will the data be collected/generated/created? | Data is generated using specialized software for controlling analytical instrumentation. |
| Will you use preexisting data? | OCAD, NIST databases, scientific literature |
| Data format | For example: pdf, JSON/HDF5/XML, CSV, ASCII, dxf and, TIFF, raw formats |
| Tools required for accessing/using the data | MS Office (spreadsheets, text documents, graphics). Instrument software is used for data processing. |
| To whom might your data be useful outside of EMBRACE? | First responders, research laboratories working with biotoxins, OPCW, UNSGM |
| Does this data asset include any personal data? | No |
| What personal data will be? | |
| What categories of persons will be included? | |
| What specific data protection requirements apply? | |
| Will you use anonymisation techniques to protect personal data? | |
| Do you comply with the requirements for valid consent? | |
| Where and how will the data be stored? | Data created by VER will be stored in computers and servers, which are controlled, authorized, and backed up by University of Helsinki. |
| Which partner will be responsible for controlling access to this data? | VER |
| How will the provenance of the data be ensured? | |
| Will you use access control and/or encryption measures to protect this data? | Yes |
| Will the data be open and reusable? | Partly. Any publications will be open access. |
| Will this data be used for further scientific research? | Yes |
| Will you use any metadata? If yes: which schema are you using? | No |

| | |
|---|---|
| Will you use any controlled vocabularies (terminologies, taxonomies, code lists), if so, which? | No |

| Question | T4.6_1 |
|---|---|
| Lead Organisation | BIOT |
| Data title | Imaging data |
| Short description | The in vitro cultured human brain cells (neural progenitor cells) and/or spheroids will be tested for specific marker expressions before sending them to MUG for biotoxin testing. This data will be generated by a high-content imaging (HCI) system. |
| Other partners involved | MUG and all partners involved in T4.6 |
| How will the data be collected/generated/created? | Data will be saved as tif files from the software of the machine and stored on BIOT's server. |
| Will you use preexisting data? | No |
| Data format | tif (png) |
| Tools required for accessing/using the data | The HCI instrument's software, image analysis software (Fiji or ImageJ). |
| To whom might your data be useful outside of EMBRACE? | The data can be part of a joint publication (together with MUG) |
| Does this data asset include any personal data? | No |
| What personal data will be? | |
| What categories of persons will be included? | |
| What specific data protection requirements apply? | |
| Will you use anonymisation techniques to protect personal data? | |
| Do you comply with the requirements for valid consent? | |
| Where and how will the data be stored? | Data will be stored on BIOT server in a specific EMBRACE project folder. Only the researchers who are working on the project and the quality management team of BIOT have access to the generated data. The generated data does not require the use of any data encryption software. |
| Which partner will be responsible for controlling access to this data? | BIOT |
| How will the provenance of the data be ensured? | |
| Will you use access control and/or encryption measures to protect this data? | No |
| Will the data be open and reusable? | The data and generated results from the data can be shared with the partners involved in WP4. |

| | |
|---|---|
| Will this data be used for further scientific research? | Yes, for publication purposes within Embrace. |
| Will you use any metadata? If yes: which schema are you using? | No |
| Will you use any controlled vocabularies (terminologies, taxonomies, code lists), if so, which? | No |

| Question | T4.6_2 |
|---|---|
| Lead Organisation | BIOT |
| Data title | qPCR data |
| Short description | The in vitro cultured human brain cells (neural progenitor cells) and/or spheroids will be tested for specific gene expressions before sending them to MUG for biotoxin testing. This data will be generated by a quantitative real-time PCR (q-rtPCR) system. |
| Other partners involved | MUG and all partners involved in T4.6, D4.6 |
| How will the data be collected/generated/created? | Data wil be saved as .rex, .xlsx files from the software of the machine and stored on BIOT's server. |
| Will you use preexisting data? | No |
| Data format | .rex, .xlsx |
| Tools required for accessing/using the data | The qPCR instrument's software, and Microsoft Excel for data analysis. |
| To whom might your data be useful outside of EMBRACE? | The data can be part of a joint publication (together with MUG). |
| Does this data asset include any personal data? | No |
| What personal data will be? | |
| What categories of persons will be included? | |
| What specific data protection requirements apply? | |
| Will you use anonymisation techniques to protect personal data? | |
| Do you comply with the requirements for valid consent? | |
| Where and how will the data be stored? | Data will be stored on BIOT server in a specific EMBRACE project folder. Only the researchers who are working on the project and the quality management team of BIOT have access to the generated data. The generated data does not require the use of any data encryption software. |
| Which partner will be responsible for controlling access to this data? | BIOT |
| How will the provenance of the data be ensured? | |
| Will you use access control and/or encryption measures to protect this data? | No |
| Will the data be open and reusable? | The data and generated results from the data can be shared with the partners involved in WP4. |

| | |
|---|---|
| Will this data be used for further scientific research? | Yes, for publication purposes within Embrace. |
| Will you use any metadata? If yes: which schema are you using? | No |
| Will you use any controlled vocabularies (terminologies, taxonomies, code lists), if so, which? | No |

## WP5. Biotoxin escalation pathway and first responder wellbeing

| Question | T5.1 |
|---|---|
| Lead Organisation | PRO |
| Data title | Casualty Care Chain Database |
| Short description | Tag & Trace casualty tracking system manages the users which can enter, edit and observe the casualties registered at an incident scene. |
| Other partners involved | |
| How will the data be collected/generated/created? | User input through mobile app |
| Will you use preexisting data? | The tag & trace application exists and is owned by PRO |
| Data format | sql |
| Tools required for accessing/using the data | user credentials and correct role |
| To whom might your data be useful outside of EMBRACE? | Customers |
| Does this data asset include any personal data? | Yes the data of the users and the casualties entered into the system |
| What personal data will be? | Name, Role, Age, Height, Weight, Location |
| What categories of persons will be included? | First responders and casualties |
| What specific data protection requirements apply? | GDPR |
| Will you use anonymisation techniques to protect personal data? | The personal information for the FTX participants can be anonymised |
| Do you comply with the requirements for valid consent? | Yes |
| Where and how will the data be stored? | Company servers |
| Which partner will be responsible for controlling access to this data? | PRO |
| How will the provenance of the data be ensured? | |
| Will you use access control and/or encryption measures to protect this data? | Role access and user credentials |
| Will the data be open and reusable? | Yes, the anonymised data can be shared |
| Will this data be used for further scientific research? | Yes |
| Will you use any metadata? If yes: which schema are you using? | No |

| | |
|---|---|
| Will you use any controlled vocabularies (terminologies, taxonomies, code lists), if so, which? | No |

| Question | T5.2 |
|---|---|
| Lead Organisation | PRO |
| Data title | Alerting Module and Source Estimation |
| Short description | This is a program which analyses the tag and trace casualty and forensics data and applies logic to it to attempt to determine relevant alerts for casualties and source of the contamination for forensics. |
| Other partners involved | |
| How will the data be collected/generated/created? | Automated process based on other system inputs |
| Will you use preexisting data? | tag & trace casualty and forensics, owned by PRO |
| Data format | json |
| Tools required for accessing/using the data | user credentials and role |
| To whom might your data be useful outside of EMBRACE? | |
| Does this data asset include any personal data? | The casualty personal data is used to provide an alert about a specific casualty |
| What personal data will be? | Name, weight, vital signs, age, height, location |
| What categories of persons will be included? | Casualties |
| What specific data protection requirements apply? | GDPR |
| Will you use anonymisation techniques to protect personal data? | Yes |
| Do you comply with the requirements for valid consent? | Yes |
| Where and how will the data be stored? | Secure company servers |
| Which partner will be responsible for controlling access to this data? | PRO |
| How will the provenance of the data be ensured? | |
| Will you use access control and/or encryption measures to protect this data? | User credentials and roles |
| Will the data be open and reusable? | Yes the anonymised data can be shared |
| Will this data be used for further scientific research? | Yes |
| Will you use any metadata? If yes: which schema are you using? | No |

| | |
|---|---|
| Will you use any controlled vocabularies (terminologies, taxonomies, code lists), if so, which? | Unknown, CAS number |

| Question | T5.3 |
|---|---|
| Lead Organisation | PRO |
| Data title | Thermal Durability Index |
| Short description | This software model predicts the durability of people based about vital signs, activity and clothing worn |
| Other partners involved | MUG |
| How will the data be collected/generated/created? | Sensor input, manual spreadsheet input |
| Will you use preexisting data? | |
| Data format | json |
| Tools required for accessing/using the data | Input through spreadsheet and results a printed to a file for reading |
| To whom might your data be useful outside of EMBRACE? | PPE manufacturers |
| Does this data asset include any personal data? | Name or ID is not required but Sex, age, weight and height are required inputs |
| What personal data will be? | |
| What categories of persons will be included? | First responder |
| What specific data protection requirements apply? | |
| Will you use anonymisation techniques to protect personal data? | |
| Do you comply with the requirements for valid consent? | |
| Where and how will the data be stored? | Company secured servers |
| Which partner will be responsible for controlling access to this data? | PRO |
| How will the provenance of the data be ensured? | |
| Will you use access control and/or encryption measures to protect this data? | URL and token access |
| Will the data be open and reusable? | Yes the data can be shared |
| Will this data be used for further scientific research? | Yes |
| Will you use any metadata? If yes: which schema are you using? | No |
| Will you use any controlled vocabularies (terminologies, taxonomies, code lists), if so, which? | No |

## WP6. Validation trials and intersectoral inter-operability

| Question | T6.4 |
|---|---|
| Lead Organisation | DCNA |
| Data title | Evaluation results |
| Short description | We will collect the feedback and evaluate the solutions during the trials. The summary of the results goes into the evaluation report. |
| Other partners involved | all partners |
| How will the data be collected/generated/created? | Feedback during trials / measurements |
| Will you use preexisting data? | no |
| Data format | text file |
| Tools required for accessing/using the data | no tools required |
| To whom might your data be useful outside of EMBRACE? | everyone interested in the solutions developed within EMBRACE |
| Does this data asset include any personal data? | yes |
| What personal data will be? | name, organisation, role -> list of participation |
| What categories of persons will be included? | many different: first responders, actors, technology providers, etc. |
| What specific data protection requirements apply? | they data shall not be published, they will not be part of the evaluation report |
| Will you use anonymisation techniques to protect personal data? | We will not publish names, we will just make a participation list for our own use |
| Do you comply with the requirements for valid consent? | yes |
| Where and how will the data be stored? | We use our own repository (Microsoft One Drive) or the one recommended/provided by the project |
| Which partner will be responsible for controlling access to this data? | DCNA |
| How will the provenance of the data be ensured? | |
| Will you use access control and/or encryption measures to protect this data? | not planned. we can add an additional password if required |
| Will the data be open and reusable? | the evaluation report will be public, but we will not publish personal data in this report |
| Will this data be used for further scientific research? | I don't know |

| | |
|---|---|
| Will you use any metadata? If yes: which schema are you using? | no |
| Will you use any controlled vocabularies (terminologies, taxonomies, code lists), if so, which? | no |

| Question | T6.5 |
|---|---|
| Lead Organisation | IANUS |
| Data title | Biotoxin Incident Response Validation Data |
| Short description | Dataset containing results and analyses from field trials and simulations to validate response strategies and risk assessment frameworks for biotoxin incidents as part of the EMBRACE project. This includes performance metrics of detection devices, effectiveness of protective gear, and responder coordination. |
| Other partners involved | TEL, DCNA, ARC, PUI, RAN |
| How will the data be collected/generated/created? | simulations and workshops |
| Will you use preexisting data? | yes if available from sources and preexisting data |
| Data format | csv, json, pdf |
| Tools required for accessing/using the data | software tools |
| To whom might your data be useful outside of EMBRACE? | Governmental emergency management agencies, academic researchers, NGOs |
| Does this data asset include any personal data? | yes assuming collecting data from field trials |
| What personal data will be? | names and roles |
| What categories of persons will be included? | emergency responders, public health officials, researchers, |
| What specific data protection requirements apply? | data is used only for the specified purposes, |
| Will you use anonymisation techniques to protect personal data? | yes |
| Do you comply with the requirements for valid consent? | yes |
| Where and how will the data be stored? | Cloud Service (Microsoft365, Hetzner) |
| Which partner will be responsible for controlling access to this data? | IANUS |
| How will the provenance of the data be ensured? | |
| Will you use access control and/or encryption measures to protect this data? | role-based access |
| Will the data be open and reusable? | reusable in terms of analysis and results |
| Will this data be used for further scientific research? | not everything |

| | |
|---|---|
| Will you use any metadata? If yes: which schema are you using? | N/A |
| Will you use any controlled vocabularies (terminologies, taxonomies, code lists), if so, which? | Yes, EPA and ISO |

## WP7. Design and implementation of the Biotoxin Reference and Stakeholder Hub

| Question | T7.1 |
|---|---|
| Lead Organisation | IANUS |
| Data title | Architecture and requirements data |
| Short description | This dataset encompasses the fundamental requirements and architectural frameworks for the development of the EMBRACE hub, including stakeholder inputs, platform requirements, architectural designs, database structures, and user interface designs. |
| Other partners involved | ARC, PUI, TEL, RAN, DCNA, VER, MUG, SMU, PRO, LC, TPEB |
| How will the data be collected/generated/created? | Surveys and interactive sessions |
| Will you use preexisting data? | SQL databases for backend structures, JavaScript and React for frontend development, |
| Data format | JSON for data interchange, SQL for structured database queries, |
| Tools required for accessing/using the data | QL Server for database management, Adobe XD |
| To whom might your data be useful outside of EMBRACE? | governmental bodies responsible for public health and safety |
| Does this data asset include any personal data? | No |
| What personal data will be? | |
| What categories of persons will be included? | |
| What specific data protection requirements apply? | |
| Will you use anonymisation techniques to protect personal data? | |
| Do you comply with the requirements for valid consent? | |
| Where and how will the data be stored? | microsoft365 |
| Which partner will be responsible for controlling access to this data? | IANUS |
| How will the provenance of the data be ensured? | |
| Will you use access control and/or encryption measures to protect this data? | Users can only access data necessary for their function |
| Will the data be open and reusable? | If needed, after the stabilization phase of the platform |

| | |
|---|---|
| Will this data be used for further scientific research? | Yes, regarding the requirements |
| Will you use any metadata? If yes: which schema are you using? | n/a |
| Will you use any controlled vocabularies (terminologies, taxonomies, code lists), if so, which? | Probably |

| Question | T7.4 |
|---|---|
| Lead Organisation | IANUS |
| Data title | SYSTEM INTEGRATION DATA |
| Short description | This dataset involves integration logs, test results, and configuration data for integrating and harmonizing the various components of the BRSH. It includes data flows between modules, authentication logs, user access records, and system scalability tests to ensure seamless functionality and robust security across the platform. |
| Other partners involved | TEL |
| How will the data be collected/generated/created? | system integration testing, including automated and manual tests |
| Will you use preexisting data? | open-source libraries and frameworks that support modular integration (RESTAPIs) |
| Data format | JSON, XML, SQL |
| Tools required for accessing/using the data | MongoDB |
| To whom might your data be useful outside of EMBRACE? | developers and engineers |
| Does this data asset include any personal data? | |
| What personal data will be? | |
| What categories of persons will be included? | |
| What specific data protection requirements apply? | |
| Will you use anonymisation techniques to protect personal data? | |
| Do you comply with the requirements for valid consent? | |
| Where and how will the data be stored? | Hetzner , Microsoft365 |
| Which partner will be responsible for controlling access to this data? | IANUS |
| How will the provenance of the data be ensured? | |
| Will you use access control and/or encryption measures to protect this data? | Yes |
| Will the data be open and reusable? | if needed |

| | |
|---|---|
| Will this data be used for further scientific research? | no |
| Will you use any metadata? If yes: which schema are you using? | n/a |
| Will you use any controlled vocabularies (terminologies, taxonomies, code lists), if so, which? | Yes, upon agreement |

## WP8. Valorisation, Sustainability and Foresight

| Question | T8.2 |
|---|---|
| Lead Organisation | LC |
| Data title | Website data collection |
| Short description | Among the types of Personal Data that this Website collects, by itself or through third parties, there are: Trackers; Usage Data. More information available: https://embracebiotoxhub.eu/privacy |
| Other partners involved | |
| How will the data be collected/generated/created? | Via acceptance of the website's terms and conditions |
| Will you use preexisting data? | No |
| Data format | Trackers; Usage Data |
| Tools required for accessing/using the data | Matomo analytics |
| To whom might your data be useful outside of EMBRACE? | N/A |
| Does this data asset include any personal data? | |
| What personal data will be? | |
| What categories of persons will be included? | |
| What specific data protection requirements apply? | |
| Will you use anonymisation techniques to protect personal data? | |
| Do you comply with the requirements for valid consent? | |
| Where and how will the data be stored? | The Data is processed at the Owner's operating offices and in any other places where the parties involved in the processing are located. |
| Which partner will be responsible for controlling access to this data? | LC |
| How will the provenance of the data be ensured? | |
| Will you use access control and/or encryption measures to protect this data? | No |
| Will the data be open and reusable? | No |
| Will this data be used for further scientific research? | No |

| | |
|---|---|
| Will you use any metadata? If yes: which schema are you using? | No |
| Will you use any controlled vocabularies (terminologies, taxonomies, code lists), if so, which? | No |

| Question | T8.3 |
|---|---|
| Lead Organisation | TPEB CR |
| Data title | Standardization Landscape as part of the Standardization Roadmap (D 8.2) |
| Short description | An overview of standards relevant to the scope of the project on which we will build further standardization activities and the Standardization Roadmap, in general |
| Other partners involved | CAS, UNMS SR, RAN |
| How will the data be collected/generated/created? | We will use our access as NSB to CEN/CENELEC and ISO/ETSI standards database |
| Will you use preexisting data? | CEN/CENELEC and ISO/ETSI standards database |
| Data format | text |
| Tools required for accessing/using the data | our in-house software as NSB |
| To whom might your data be useful outside of EMBRACE? | anyone in the CBRNe community interested in the standardization aspect |
| Does this data asset include any personal data? | No |
| What personal data will be? | N/A |
| What categories of persons will be included? | N/A |
| What specific data protection requirements apply? | N/A |
| Will you use anonymisation techniques to protect personal data? | N/A |
| Do you comply with the requirements for valid consent? | N/A |
| Where and how will the data be stored? | In the CAS internal system, this data does not need special protection beyond the scope of our internal policies |
| Which partner will be responsible for controlling access to this data? | CAS, UNMS SR |
| How will the provenance of the data be ensured? | |
| Will you use access control and/or encryption measures to protect this data? | no |
| Will the data be open and reusable? | we will be sharing the outcome - i.e. the Standardization Roadmap, which will contain identification and scope of relevant standards, however, we cannot share full documents |

| | |
|---|---|
| Will this data be used for further scientific research? | no |
| Will you use any metadata? If yes: which schema are you using? | no |
| Will you use any controlled vocabularies (terminologies, taxonomies, code lists), if so, which? | yes - ISO and CEN/CENELEC |

| Question | T2.4 |
|---|---|
| Lead Organisation | VER |
| Data title | Training material |
| Short description | New training material will be create and add to the CBRN toolbox |
| Other partners involved | PCNA, MUG and PUI |
| How will the data be collected/generated/created? | Filming, taking photos, etc |
| Will you use preexisting data? | Not at the moment |
| Data format | Mostly pdf, jpeg and mpeg |
| Tools required for accessing/using the data | Web browser and corresponding software (e.g. pdf reader) |
| To whom might your data be useful outside of EMBRACE? | Mainly first responders |
| Does this data asset include any personal data? | no |
| What personal data will be? | nada |
| What categories of persons will be included? | nada |
| What specific data protection requirements apply? | username and password |
| Will you use anonymisation techniques to protect personal data? | no |
| Do you comply with the requirements for valid consent? | No personal data, so GDPR won't apply |
| Where and how will the data be stored? | Helsinki university server, data is stored in server's hard drives and random access memory (RAM) when needed. |
| Which partner will be responsible for controlling access to this data? | VER |
| How will the provenance of the data be ensured? | |
| Will you use access control and/or encryption measures to protect this data? | Username and password |
| Will the data be open and reusable? | Data is available if username and password is known |
| Will this data be used for further scientific research? | Yes |
| Will you use any metadata? If yes: which schema are you using? | No |
| Will you use any controlled vocabularies (terminologies, taxonomies, code lists), if so, which? | No |